

CLAIMS

1-50. (cancelled)

51. (new) A method of thwarting detection of a secret binary number in a cryptographic computational device by analysis of externally observable parameters, comprising:

conditionally performing a plurality of calculations in response to the bit values of said

secret number;

multiplicatively accumulating the results of said plurality of calculations in a subtotal; and

performing dummy calculations in response to selected bit positions of said secret

number that indicate calculations should not be performed, and not

multiplicatively accumulating the results of the dummy calculations in said

subtotal;

whereby said dummy calculations alter at least one externally observable parameter.

52. (new) The method of claim 51 wherein conditionally performing a plurality of calculations in response to the bit values of said secret number comprises performing a calculation where said bit value is a one and not performing said calculation where said bit value is a zero.

53. (new) The method of claim 52 wherein performing dummy calculations in response to selected bit positions of said secret number that indicate calculations should not be performed comprises performing said dummy calculations in response to selected ones of said secret number bit positions whose bit value is zero.

54. (new) The method of claim 53 wherein said selected ones of said secret number bit positions whose bit value is zero are identified by an indicator in the form of a binary word

having a length equal to that of said secret number and having a bit value of one in a select number of places that said secret number has a bit value of zero.

55. (new) The method of claim 54 wherein the bit values of one in said indicator are randomly distributed over the places that the secret number has a bit value of zero.

56. (new) The method of claim 53 wherein said indicator is fixed.

57. (new) The method of claim 56 wherein said indicator is generated upon first commissioning said device into operation and internally storing said indicator such that it is never released outside said device.

58. (new) The method of claim 51 further comprising generating said secret number upon first commissioning said device into operation and internally storing said secret number such that it is never released outside said device.

59. (new) The method of claim 51 in which said externally observable parameters include variation in power supply current.

60. (new) The method of claim 51 in which said externally observable parameters include variation in timing of outputting results of said calculations.

61. (new) The method of claim 51 wherein conditionally performing a plurality of calculations and accumulating their results calculates the exponentiation of a long integer to the power of a large secret exponent.

62. (new) The method of claim 61 in which calculating the exponentiation of a long integer to the power of a large secret exponent comprises selectively calculating successive squares of said long integer and multiplicatively accumulating said squares in response to the bit values of said secret exponent, and reducing said accumulated value modulo a given modulus.

63. (new) A method of thwarting detection of a large, secret binary exponent in a cryptographic computational device executing the operation of exponentiating a long integer to the power of said secret exponent, the detection being by analysis of externally observable parameters of said device, comprising:

- calculating successive squares of said long integer in a group of a predetermined size and temporarily storing the results, said calculations altering at least one said externally observable parameter; and

- multiplicatively accumulating selected ones of the results of said plurality of calculations in response to a corresponding group of bit values of said secret exponent, said selection of results to be accumulated not substantially altering an externally observable parameter.

64. (new) The method of claim 63 wherein selectively multiplicatively accumulating selected ones of the results of said plurality of calculations in response to a corresponding group of bit values of said secret exponent comprises multiplicatively accumulating each said result if the corresponding bit value of said secret exponent is a one, and not multiplicatively accumulating each said result if the corresponding bit value of said secret exponent is a zero.

65. (new) The method of claim 63 wherein said predetermined size is the bit length of said secret binary exponent.

66. (new) The method of claim 63 further comprising recalculating each said successive square in said group, regardless of whether said square was multiplicatively accumulated, using values for the corresponding successive square of the next said group of bit values.

67. (new) A method of thwarting detection of a large, secret binary exponent in a cryptographic computational device executing the operation of exponentiating a long integer to the power of said secret exponent, the detection being by analysis of externally observable parameters of said device, comprising:

factoring said secret exponent into a product of sparse binary integers plus a remainder such that the total number of ones in said sparse integers and said remainder together is a minimum;

exponentiating said long integer to the power of one of said sparse binary integers to obtain a first intermediate result;

exponentiating said first intermediate result to the power of the other said sparse binary integer to obtain a second intermediate result;

exponentiating said long integer to the power of said remainder to obtain a third intermediate result; and

multiplying said second intermediate result and said third intermediate result and modulo-reducing the product by a given modulus;

whereby said exponentiation operations alter at least one said externally observable parameter in a different manner than would the exponentiation of said long integer by said secret exponent.

68. (new) The method of claim 67 further wherein factoring said secret exponent into a product of sparse binary integers plus a remainder is performed once upon first commissioning said

device into operation and further comprising internally storing said sparse binary integers and said remainder such that they are never released outside said device.

69. (new) The method of claim 67 wherein each said exponentiation operation comprises selectively calculating successive squares of the base and multiplicatively accumulating them in response to a corresponding bit value of one in the exponent.

70. (new) The method of claim 69 further comprising performing dummy calculations in response to selected bit positions of said exponent having a bit value of zero, and not multiplicatively accumulating the results of the dummy calculations.

71. (new) The method of claim 70 wherein said selected bit positions of said exponent having a bit value of zero are identified by an indicator in the form of a binary word having a length equal to that of said exponent and having a bit value of one in a select number of places that said exponent has a bit value of zero.

72. (new) The method of claim 69 further comprising:

calculating successive squares of said base in a group of a predetermined size and

temporarily storing the results; and

multiplicatively accumulating selected ones of the results of said plurality of calculations

in response to a corresponding group of bit values of said secret exponent.

73. (new) A detection-proof computational device comprising:

an input/output interface;

a memory storing a secret binary number; and

a processor operatively connected to said input/output interface and to said memory and programmed for cryptographic computation using said secret binary number while thwarting detection of said secret binary number by analysis of externally observable parameters, the cryptographic computation comprising:
conditionally performing a plurality of calculations in response to the bit values of said secret number;
multiplicatively accumulating the results of said plurality of calculations in a subtotal; and
performing dummy calculations in response to selected bit positions of said secret number that indicate calculations should not be performed, and not multiplicatively accumulating the results of the dummy calculations in said subtotal;
whereby said dummy calculations alter at least one externally observable parameter.

74. (new) The device of claim 73, said memory further storing an indicator in the form of a binary word having a length equal to that of said secret binary number and having a bit value of one in a select number of places that the secret number has a bit value of zero.

75. (new) The device of claim 73 wherein said select positions of said indicator having a bit value of one are randomly selected.

76. (new) The device of claim 73 in which in which said externally observable parameters include variation in power supply current.

77. (new) The device of claim 73 in which said externally observable parameters include variation in timing of outputting results of said calculations.

78. (new) The device of claim 73 wherein said secret cryptographic computations comprise exponentiating a long integer to the power of a large secret exponent.

79. (new) The device of claim 78 wherein exponentiating a long integer to the power of a large secret exponent comprises selectively calculating successive squares of said long integer and multiplicatively accumulating said squares in response to the bit values of said secret exponent, and reducing said accumulated value modulo a given modulus.

80. (new) A secure computational device comprising:

an input/output interface receiving a long integer;

a memory storing a secret exponent; and

a processor operatively connected to said input/output interface and to said memory and

programmed for the cryptographic computation of exponentiating said long integer to the power of said secret exponent, while thwarting detection of said secret exponent by analysis of externally observable parameters, the cryptographic computation comprising:

calculating successive squares of said long integer in a group of a predetermined

size and temporarily storing the results, said calculations altering at least one said externally observable parameter; and

multiplicatively accumulating selected ones of the results of said plurality of calculations in response to a corresponding group of bit values of said secret exponent, said selection of results to be accumulated not substantially altering an externally observable parameter.

81. (new) The device of claim 80 wherein selectively multiplicatively accumulating selected ones of the results of said plurality of calculations in response to a corresponding group of bit values of said secret exponent comprises multiplicatively accumulating each said result if the corresponding bit value of said secret exponent is a one, and not multiplicatively accumulating each said result if the corresponding bit value of said secret exponent is a zero.

82. (new) The device of claim 80 wherein said predetermined size is the bit length of said secret binary exponent.

83. (new) The device of claim 80 further wherein said processor further recalculates each said successive square in said group, regardless of whether said square was multiplicatively accumulated, using values for the corresponding successive square of the next said group of bit values.

84. (new) The device of claim 80 wherein said device comprises a smart card.

85. (new) A secure computational device comprising:

- an input/output interface receiving a long integer;

- a memory storing a secret exponent; and

- a processor operatively connected to said input/output interface and to said memory and programmed for the cryptographic computation of exponentiating said long integer to the power of said secret exponent, while thwarting detection of said secret exponent by analysis of externally observable parameters, the cryptographic computation comprising:

factoring said secret exponent into a product of sparse binary integers plus a remainder such that the total number of ones in said sparse integers and said remainder together is a minimum;

exponentiating said long integer to the power of one of said sparse binary integers to obtain a first intermediate result;

exponentiating said first intermediate result to the power of the other said sparse binary integer to obtain a second intermediate result;

exponentiating said long integer to the power of said remainder to obtain a third intermediate result; and

multiplying said second intermediate result and said third intermediate result and modulo-reducing the product by a given modulus;

whereby said exponentiation operations alter at least one said externally observable parameter in a different manner than would the exponentiation of said long integer by said secret exponent.

86. (new) The device of claim 85 wherein factoring said secret exponent into a product of sparse binary integers plus a remainder is performed once upon first commissioning said device into operation and further comprising internally storing said sparse binary integers and said remainder such that they are never released outside said device.

87. (new) The device of claim 85 wherein each said exponentiation operation comprises selectively calculating successive squares of the base and multiplicatively accumulating them in response to a corresponding bit value of one in the exponent, and reducing said accumulated value modulo a given modulus.

88. (new) A mobile terminal used in a mobile communications system comprising:

a transmitter and a receiver for communicating in the mobile communications system;

a controller controlling operation of the transmitter and the receiver; and

a secure device removably, operatively connectable to the controller and comprising:

an input/output interface;

a memory storing a secret binary number; and

a processor operatively connected to said input/output interface and to said

memory and programmed for cryptographic computation using said

secret binary number while thwarting detection of said secret binary

number by analysis of externally observable parameters, the

cryptographic computation comprising:

conditionally performing a plurality of calculations in response to the bit

values of said secret number;

multiplicatively accumulating the results of said plurality of calculations in

a subtotal; and

performing dummy calculations in response to selected bit positions of

said secret number that indicate calculations should not be

performed, and not multiplicatively accumulating the results of the

dummy calculations in said subtotal;

whereby said dummy calculations alter at least one externally observable

parameter.

89. (new) The mobile terminal of claim 88, said memory further storing an indicator in the form of a binary word having a length equal to that of said secret binary number and having a bit value of one in a select number of places that the secret number has a bit value of zero.

90. (new) The mobile terminal of claim 88 wherein said select positions of said indicator having a bit value of one are randomly selected.

91. (new) The mobile terminal of claim 88 in which in which said externally observable parameters include variation in power supply current.

92. (new) The mobile terminal of claim 88 in which said externally observable parameters include variation in timing of outputting results of said calculations.

93. (new) The mobile terminal of claim 88 wherein said secret cryptographic computations comprise exponentiating a long integer to the power of a large secret exponent.

94. (new) The mobile terminal of claim 93 wherein exponentiating a long integer to the power of a large secret exponent comprises selectively calculating successive squares of said long integer and multiplicatively accumulating said squares in response to the bit values of said secret exponent, and reducing said accumulated value modulo a given modulus.

95. (new) A mobile terminal used in a mobile communications system comprising:

- a transmitter and a receiver for communicating in the mobile communications system;
- a controller controlling operation of the transmitter and the receiver; and
- a secure device removably, operatively connectable to the controller and comprising:
 - an input/output interface receiving a long integer;
 - a memory storing a secret exponent; and
 - a processor operatively connected to said input/output interface and to said memory and programmed for the cryptographic computation of exponentiating said long integer to the power of said secret exponent,

while thwarting detection of said secret exponent by analysis of externally observable parameters, the cryptographic computation comprising:
calculating successive squares of said long integer in a group of a predetermined size and temporarily storing the results, said calculations altering at least one said externally observable parameter; and
multiplicatively accumulating selected ones of the results of said plurality of calculations in response to a corresponding group of bit values of said secret exponent, said selection of results to be accumulated not substantially altering an externally observable parameter.

96. (new) The mobile terminal of claim 95 wherein selectively multiplicatively accumulating selected ones of the results of said plurality of calculations in response to a corresponding group of bit values of said secret exponent comprises multiplicatively accumulating each said result if the corresponding bit value of said secret exponent is a one, and not multiplicatively accumulating each said result if the corresponding bit value of said secret exponent is a zero.

97. (new) The mobile terminal of claim 95 wherein said predetermined size is the bit length of said secret binary exponent.

98. (new) The mobile terminal of claim 95 wherein said processor further recalculates each said successive square in said group, regardless of whether said square was multiplicatively accumulated, using values for the corresponding successive square of the next said group of bit values.

99. (new) A mobile terminal used in a mobile communications system comprising:

a transmitter and a receiver for communicating in the mobile communications system;

a controller controlling operation of the transmitter and the receiver; and

a secure device removably, operatively connectable to the controller and comprising:

an input/output interface receiving a long integer;

a memory storing a secret exponent; and

a processor operatively connected to said input/output interface and to said

memory and programmed for the cryptographic computation of

exponentiating said long integer to the power of said secret exponent,

while thwarting detection of said secret exponent by analysis of externally
observable parameters, the cryptographic computation comprising:

factoring said secret exponent into a product of sparse binary integers

plus a remainder such that the total number of ones in said sparse
integers and said remainder together is a minimum;

exponentiating said long integer to the power of one of said sparse binary
integers to obtain a first intermediate result;

exponentiating said first intermediate result to the power of the other said
sparse binary integer to obtain a second intermediate result;

exponentiating said long integer to the power of said remainder to obtain
a third intermediate result; and

multiplying said second intermediate result and said third intermediate
result and modulo-reducing the product by a given modulus;

whereby said exponentiation operations alter at least one said externally
observable parameter in a different manner than would the
exponentiation of said long integer by said secret exponent.

100. (new) The mobile terminal of claim 99 wherein factoring said secret exponent into a product of sparse binary integers plus a remainder is performed once upon first commissioning said device into operation and further comprising internally storing said sparse binary integers and said remainder such that they are never released outside said device.

101. (new) The mobile terminal of claim 99 wherein each said exponentiation operation comprises selectively calculating successive squares of the base and multiplicatively accumulating them in response to a corresponding bit value of one in the exponent, and reducing said accumulated value modulo a given modulus.

102. (new) The mobile terminal of claim 99 wherein said device comprises a smart card.

103. (new) The mobile terminal of claim 99 wherein said device comprises a subscriber identity module.